IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Application of:		Atty. Docket No.:	004770.00521
	Janne Suuronen *et al.*		
Serial No.:	10/059,182	Group Art Unit:	2439
Filed:	January 31, 2002	Examiner:	Yin Chen Shaw
For:	System and Method of Providing Virus Protection At A Gateway	Confirmation No.:	5357

APPEAL BRIEF

U.S. Patent and Trademark Office
Customer Service Window
Mail Stop - Appeal
Randolph Building
401 Dulany Street
Alexandria, VA 22314

Sir:

This is an Appeal Brief filed in support of the Notice of Appeal filed July 21, 2010. Appeal is taken from the Final Office Action mailed May 11, 2010.

General Authorization of Payment of Fees

If any fees are due, or if any overpayments have been made, whether or not associated with this filing, please debit or credit Deposit Account No. 19-0733, accordingly. Any necessary extensions of time are hereby requested.

REAL PARTY IN INTEREST
37 C.F.R. § 41.37(c)(1)(i)

The owner of this application, and the real party in interest, is Nokia Corporation, of Espoo, Finland.

RELATED APPEALS AND INTERFERENCES
37 C.F.R. § 41.37(c)(1)(ii)

There are no known related appeals or interferences.

STATUS OF CLAIMS
37 C.F.R. § 41.37(c)(1)(iii)

Claims 1, 4-6, 11, 32-34, 40-50, 53, 54, 56-63, and 65 are pending and rejected. Claims 2, 3, 7-10, 12-31, 35-39, 51, 52, 55, and 64 were previously cancelled without prejudice or disclaimer. Appellant hereby appeals the rejection of the pending claims.

STATUS OF AMENDMENTS
37 C.F.R. § 41.37(c)(1)(iv)

There are no outstanding amendments, as the status of the claims provided herein is indicative of the claims on appeal.

SUMMARY OF CLAIMED SUBJECT MATTER
37 C.F.R. § 41.37(c)(1)(v)

In making reference herein to various embodiments in the specification text and/or drawings to explain the claimed invention, Appellant does not intend to limit the claims to those embodiments; all references to the specification and drawings are illustrative unless otherwise explicitly stated. Appellant refers to the filed specification at the cited passages for support with the understanding that the specification, when taken as a whole, also provides support.

Independent claim 1 is directed to an apparatus comprising a firewall. Specification, paragraphs [0005], [0007]-[0009], [0017]; Figure 1 (gateway 12 including firewall 14). The firewall is configured to receive data packets over a first network. Specification, paragraphs [0007]-[0009], [0017]; Figure 1 (first network 11). The firewall is further configured to classify the received data packets based on the contents of the data packets into packets of a first type which cannot contain a virus and packets of a second type which can contain a virus. Specification, paragraphs [0007]-[0009], [0017], [0018]; Figure 1 (packet classification database 16). Classifying the received data packets includes determining whether at least one of the data packets includes content for a real-time audio or video data stream. Specification, paragraphs [0007]-[0009], [0017], [0018]; Figure 1 (packet classification database 16). The firewall is further configured to forward the data packets of the first type to a destination without testing by a virus scanning engine and without transmission of the data packets to the virus scanning

engine. Specification, paragraphs [0007]-[0009], [0017], [0018]; Figure 1 (output 20). The firewall is further configured to forward the data packets of the second type to a virus scanning engine for testing. Specification, paragraphs [0007]-[0009], [0017], [0018]; Figure 1 (virus scanning engine 22).

Independent claim 49 is directed to a method comprising receiving data packets. Specification, paragraphs [0007]-[0009], [0017]. The method further comprises classifying the data packets based on the contents of the data packets into packets of a first type which cannot contain a virus and packets of a second type which can contain a virus. Specification, paragraphs [0007]-[0009], [0017], [0018]. Classifying the received data packets includes determining whether at least one of the data packets includes content for a real-time audio or video data stream. Specification, paragraphs [0007]-[0009], [0017], [0018]. The method further comprises transmitting the received data packets of the first type to a destination without testing by a virus scanning engine and without transmission of the data packets to the virus scanning engine. Specification, paragraphs [0007]-[0009], [0017], [0018]. The method further comprises transmitting the received data packets of the second type to a virus scanning engine for testing. Specification, paragraphs [0007]-[0009], [0017], [0018].

Independent claim 50 is directed to one or more non-transitory computer readable media storing computer executable instructions that, when executed, cause an apparatus to receive data packets. Specification, paragraphs [0010], [0017], [0018]; Figure 1 (gateway 12 including firewall 14). The instructions, when executed, further cause the apparatus to classify the received data packets based on the contents of the data packets into packets of a first type that cannot contain a virus and packets of a second type that can contain a virus. Specification, paragraphs [0010], [0017], [0018]; Figure 1 (packet classification database 16). Classifying the received data packets includes determining whether at least one of the data packets includes content for a real-time audio or video data stream. Specification, paragraphs [0010], [0017], [0018]; Figure 1 (packet classification database 16). The instructions, when executed, further cause the apparatus to transmit the data packets of the first type to a destination without testing by a virus scanning engine and without transmission of the data packets to the virus scanning engine. Specification, paragraphs [0010], [0017], [0018]; Figure 1 (output 20). The instructions,

when executed, further cause the apparatus to transmit the data packets of the second type to a virus scanning engine for testing. Specification, paragraphs [0010], [0017], [0018]; Figure 1 (virus scanning engine 22).

Independent claim 62 is directed to an apparatus comprising a processor and memory storing computer executable instructions that, when executed by the processor, cause the apparatus to receive data packets. Specification, paragraphs [0007], [0010], [0017], [0019]; Figure 1 (gateway 12 including firewall 14 and virus scanning engine 22). The instructions, when executed by the processor, further cause the apparatus to classify the data packets based on the contents of the data packets into packets of a first type which cannot contain a virus and packets of a second type which can contain a virus. Specification, paragraphs [0007], [0010], [0017]-[0019]; Figure 1 (packet classification database 16). Classifying the received data packets includes determining whether at least one of the data packets includes content for a real-time audio or video data stream. Specification, paragraphs [0007], [0010], [0017]-[0019]; Figure 1 (packet classification database 16). The instructions, when executed by the processor, further cause the apparatus to transmit the data packets of the first type to a destination without testing by a virus scanning engine and without transmission of the data packets to the virus scanning engine. Specification, paragraphs [0007], [0010], [0017]-[0019]; Figure 1 (output 20). The instructions, when executed by the processor, further cause the apparatus to transmit the data packets of the second type to a virus scanning engine for virus testing. Specification, paragraphs [0007], [0010], [0017]-[0019]; Figure 1 (virus scanning engine 22).

GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL
37 C.F.R. § 41.37(c)(1)(vi)

- Whether claims 1, 4, 5, 11, 32-34, 40-50, 53, 56-63, and 65 are unpatentable under 35 U.S.C. § 103(a) over Fink *et al.* (U.S. Patent No. 6,496,935, "Fink") in view of Joyce (U.S. Patent No. 6,519,703, "Joyce") and Baum *et al.* (U.S. Patent No. 6,400,707, "Baum").
- Whether claims 6 and 54 are unpatentable under 35 U.S.C. § 103(a) over Fink, Joyce, and Baum, and further in view of Lyle (U.S. Patent No. 6,886,102, "Lyle").

ARGUMENT
37 C.F.R. § 41.37(c)(1)(vii)

A. Rejection Of Claims 1, 4, 5, 11, 32-34, 40-50, 53, 56-63, And 65 Under 35 U.S.C. § 103(a) Over Fink, In View Of Joyce And Baum

1. Independent Claim 1 And Dependent Claims 4, 5, 11, 32-34, And 41-48

Independent claim 1 recites, among other features, "a firewall configured to . . . classify the received data packets based on the contents of the data packets into packets of a first type which cannot contain a virus and packets of a second type which can contain a virus, *wherein classifying the received data packets includes determining whether at least one of the data packets includes content for a real-time audio or video data stream.*"

The May 11, 2010, Final Office Action at pages 7-8 concedes that Fink and Joyce fail to teach or suggest that classifying received data packets includes determining whether at least one of the data packets includes content for a real-time audio or video data stream as recited in claim 1. The Office Action at page 8, however, contends that Baum at col. 2, lines 41-59; col. 5, lines 61-62; col. 6, lines 25-57; and col. 7, lines 20-22 describes such features. Notably, the Office Action at pages 2-3 ("Response to Arguments") asserts that Baum provides for classification by distinguishing whether a packet is data or voice, specifically citing Baum at col. 7, lines 20-22.

As discussed at pages 8-9 of the Amendment and Response filed January 26, 2010, Baum fails to teach or suggest the above-noted features recited in claim 1. Specifically, Baum's description of a rule based packet filter (col. 5, lines 61-62) fails to teach or suggest that the filter determines whether a packet includes audio or video in classifying that packet. Baum's system relates to the generation of filter parameters based on set-up signaling dialog and does not teach or suggest the consideration of whether a packet includes audio or video in classifying the packet. Baum acknowledges the existence of audio or video packets (col. 2, lines 41-59). However, Baum does not describe or suggest determining whether any particular data packet includes audio or video. Without such a teaching, Baum cannot teach classifying received data packets based on the contents of the data packets into packets of a first type which cannot contain a virus and packets of a second type which can contain a virus, wherein classifying the

received data packets includes determining whether at least one of the data packets includes content for a real-time audio or video data stream as recited in claim 1. Thus, notwithstanding whether the cited documents are properly combinable, the asserted combination would not have resulted in the features as recited in claim 1.

Claims 4, 5, 11, 32-34, and 41-48 depend from claim 1 and are distinguishable from the applied documents for at least the same reasons as claim 1, and further in view of the unique combinations of features recited therein.

2. Dependent Claim 40

Claim 40 depends from claim 1 and is distinguishable from the applied documents for at least the same reasons as claim 1.

Moreover, claim 40 recites "a virus scanning engine configured to alert *the* destination upon detection of a virus in the data packets." When claim 40 is read in connection with its parent claim 1, it is clear that the destination alerted upon the detection of a virus in the data packets is the same destination to which the data packets of the first type are forwarded. The Office Action at page 13 contends that Joyce at col. 4, lines 61-67 describes these features of claim 40. Joyce at col. 4, lines 61-67 is reproduced below:

> In the event that either of heuristic stages **46** or **48** discover problems in session data or session data flow, control is switched to an external call or alternate process **49**. Examples of external call or alternate process **49** are alarms; alerting devices; pager systems providing a message to an administrator, a security officer, or the FBI; or a log file. In one embodiment, a choice is made of any or all of these

Thus, even assuming (without admitting) that network 30 of Joyce could have been analogized to the destination recited in claims 1 and 40 (as contended at page 6 of the Office Action in rejecting claim 1), Joyce fails to describe alerting network 30 upon detection of a virus in data packets. Indeed, Joyce at col. 4, lines 61-67 merely describes switching control to external call or alternate process 49 when a problem is discovered in session data or session data flow. Switching control to an external call or alternate process 49 is different from alerting

network 30 upon a detection of a virus. Claim 40 is allowable for at least these additional reasons.

3. Independent Claim 49 And Dependent Claims 58-61

Independent claim 49 recites, among other features, "classifying the data packets based on the contents of the data packets into packets of a first type which cannot contain a virus and packets of a second type which can contain a virus, wherein classifying the received data packets includes determining whether at least one of the data packets includes content for a real-time audio or video data stream." Such features are distinguishable from the applied documents for at least reasons substantially similar to those discussed above with respect to claim 1.

Claims 58-61 depend from claim 49 and are distinguishable from the applied documents for at least the same reasons as claim 49, and further in view of the unique combinations of features recited therein.

4. Independent Claim 50 And Dependent Claims 53, 56, 57, And 65

Independent claim 50 recites, among other features, "classify the received data packets based on the contents of the data packets into packets of a first type that cannot contain a virus and packets of a second type that can contain a virus, wherein classifying the received data packets includes determining whether at least one of the data packets includes content for a real-time audio or video data stream." Such features are distinguishable from the applied documents for at least reasons substantially similar to those discussed above with respect to claim 1.

Claims 53, 56, 57, and 65 depend from claim 50 and are distinguishable from the applied documents for at least the same reasons as claim 50, and further in view of the unique combinations of features recited therein.

5. Independent Claim 62 And Dependent Claim 63

Independent claim 62 recites, among other features, "classify the data packets based on the contents of the data packets into packets of a first type which cannot contain a virus and packets of a second type which can contain a virus, wherein classifying the received data packets includes determining whether at least one of the data packets includes content for a real-time audio or video data stream." Such features are distinguishable from the applied documents for at least reasons substantially similar to those discussed above with respect to claim 1.

Claim 63 depends from claim 62 and is distinguishable from the applied documents for at least the same reasons as claim 62, and further in view of the unique combinations of features recited therein.

B. Rejection Of Claims 6 And 54 Under 35 U.S.C. § 103(a) Over Fink, Joyce, And Baum, And Further In View Of Lyle

Claims 6 and 54 depend from claims 1 and 50, respectively, and are distinguishable from the applied documents for at least the reasons discussed above with respect to claims 1 and 50, as Lyle fails to remedy the deficiencies of Fink, Joyce and Baum (notwithstanding whether the alleged combination of documents would have been proper).

CONCLUSION

For all of the foregoing reasons, Appellant respectfully submits that the standing rejections of the appealed claims are improper and should be reversed.

Respectfully submitted,

BANNER & WITCOFF, LTD.

Dated: October 4, 2010

By: /Mark E. Wilinski/
Mark E. Wilinski
Registration No. 63,230

CLAIMS APPENDIX
37 C.F.R. § 41.37(c)(1)(viii)

Claims involved in the appeal:

Claim 1: An apparatus comprising:

a firewall configured to:

receive data packets over a first network;

classify the received data packets based on the contents of the data packets into packets of a first type which cannot contain a virus and packets of a second type which can contain a virus, wherein classifying the received data packets includes determining whether at least one of the data packets includes content for a real-time audio or video data stream;

forward the data packets of the first type to a destination without testing by a virus scanning engine and without transmission of the data packets to the virus scanning engine; and

forward the data packets of the second type to a virus scanning engine for testing.

Claims 2-3: (Canceled)

Claim 4: The apparatus of claim 1, wherein the classifying comprises determining that data packets of the first type contain real time data other than the audio or video data stream.

Claim 5: The apparatus of claim 4, wherein the classifying comprises determining that data packets of the first type are part of the audio or video data stream.

Claim 6: The apparatus of claim 1, wherein the firewall is configured to stop reception of a data stream containing the data packets in response to an alert from the virus scanning engine.

Claims 7-10: (Canceled)

Claim 11: The apparatus of claim 1, further comprising a buffer configured to store the data packets of the second type while the virus scanning engine is testing the data packets to detect a virus.

Claims 12-31: (Canceled)

Claim 32: The apparatus of claim 1, wherein the firewall is configured to receive from a packet classification database information defining the first and second types of data packets.

Claim 33: The apparatus of claim 32, further comprising:

a virus scanning engine configured to receive from a virus detection database programming information controlling the testing of the data packets of the second type by the virus scanning engine.

Claim 34: The apparatus of claim 1, further comprising:

a virus scanning engine configured to receive from a virus detection database programming information controlling the testing of the data packets of the second type by the virus scanning engine.

Claims 35-39: (Canceled)

Claim 40: The apparatus of claim 1, further comprising a virus scanning engine configured to alert the destination upon detection of a virus in the data packets.

Claim 41: The apparatus of claim 1 wherein the destination is a local area network.

Claim 42: The apparatus of claim 1 wherein the destination is a personal computer.

Claim 43: The apparatus of claim 1, wherein the destination is a second network.

Claim 44: The apparatus of claim 1, wherein the first network is a wide area network.

Claim 45: The apparatus of claim 44, wherein the wide area network is the Internet.

Claim 46: The apparatus of claim 1, wherein

the destination comprises an Internet service provider configured to connect to a gateway, a modem configured to connect to the Internet service provider, and one of a local area network or personal computer configured to connect to the modem.

Claim 47: The apparatus of claim 1, further comprising a virus scanning engine configured to decode the data packets during the testing of the data packets.

Claim 48: The apparatus of claim 47, wherein the virus scanning engine is configured to function as a proxy for a destination processor configured to receive the data packets.

Claim 49: A method comprising:

receiving data packets;

classifying the data packets based on the contents of the data packets into packets of a first type which cannot contain a virus and packets of a second type which can contain a virus, wherein classifying the received data packets includes determining whether at least one of the data packets includes content for a real-time audio or video data stream;

transmitting the received data packets of the first type to a destination without testing by a virus scanning engine and without transmission of the data packets to the virus scanning engine; and

transmitting the received data packets of the second type to a virus scanning engine for testing.

Claim 50: One or more non-transitory computer readable media storing computer executable instructions that, when executed, cause an apparatus to:

receive data packets;

classify the received data packets based on the contents of the data packets into packets of a first type that cannot contain a virus and packets of a second type that can contain a virus, wherein classifying the received data packets includes determining whether at least one of the data packets includes content for a real-time audio or video data stream;

transmit the data packets of the first type to a destination without testing by a virus scanning engine and without transmission of the data packets to the virus scanning engine; and

transmit the data packets of the second type to a virus scanning engine for testing.

Claims 51-52: (Canceled)

Claim 53: The one or more non-transitory computer readable media in accordance with claim 50, wherein the classifying comprises determining that the data packets of the first type include the content for the real-time audio or video data stream.

Claim 54: The one or more non-transitory computer readable media in accordance with claim 50, wherein:

the computer program when executed causes reception of a data stream containing the data packets to be stopped in response to an alert from the virus scanning engine.

Claim 55: (Canceled)

Claim 56: The one or more non-transitory computer readable media in accordance with claim 50, wherein the computer executable instructions, when executed, further cause the apparatus to receive from a packet classification database information defining first and second types of data packets.

Claim 57: The one or more non-transitory computer readable media in accordance with claim 53, wherein the classifying further comprises determining that data packets of the first type are part of the audio or video data stream.

Claim 58: The method of claim 49, wherein the classifying comprises determining that data packets of the first type contain real time data other than the audio or video data stream.

Claim 59: The method of claim 58, wherein the classifying further comprises determining that data packets of the first type are part of the audio or video data stream.

Claim 60: The method of claim 49, further comprising receiving information from a packet classification database, said information defining the first and second types of data packets.

Claim 61: The method of claim 49, wherein the classifying is performed by a firewall.

Claim 62: An apparatus, comprising:

a processor; and

memory storing computer executable instructions that, when executed by the processor, cause the apparatus to:

receive data packets;

classify the data packets based on the contents of the data packets into packets of a first type which cannot contain a virus and packets of a second type which can contain a virus, wherein classifying the received data packets includes determining whether at least one of the data packets includes content for a real-time audio or video data stream;

transmit the data packets of the first type to a destination without testing by a virus scanning engine and without transmission of the data packets to the virus scanning engine; and

transmit the data packets of the second type to a virus scanning engine for virus testing.

Claim 63: The apparatus of claim 62, wherein the classifying comprises determining that data packets of the first type are part of the real-time audio or video data stream.

Claim 64: (Cancelled).

Claim 65: The one or more non-transitory computer readable media storing in accordance with claim 50, wherein the classification is performed by a firewall.

EVIDENCE APPENDIX
37 C.F.R. § 41.37(c)(1)(ix)

NONE.

RELATED PROCEEDINGS APPENDIX
37 C.F.R. § 41.37(c)(1)(x)

NONE.